PN - JP2000059385 A 20000225

PD - 2000-02-25

PR - JP19980224982 19980807

OPD - 1998-08-07

TI - METHOD FOR MANAGING PLURAL SYSTEMS AT TIME OF OVERLAPPING IP ADDRESSES

IN - SAKURAI YOSHIHARU

PA - NTT DATA CORP

IC - H04L12/28 ; G06F13/00 ; H04L12/56

TI - Multiple system management procedure used during internal protocol address duplication

PR - JP19980224982 19980807

PN - JP2000059385 A 20000225 DW200024 H04L12/28 011pp

PA - (NITE) NTT DATA TSUSHIN KK

IC - G06F13/00 ;H04L12/28 ;H04L12/56

AB - JP2000059385 NOVELTY - A system ID which can specify which server machine (18) is the transmission origin of the communication data is added from the server machine when communicating with a monitoring manager (19). The monitoring manager adds the system ID which can specify the server machine functioning as a transmission destination.

- USE - Used during internet protocol IP address duplication.
- ADVANTAGE - Does not need installation of manager even if duplicate IP address is utilized. Does not need special modification of correspondence to communication by expanded SNMP. Does not require user to recognize structure.
- DESCRIPTION OF DRAWING(S) - The figure is a diagram showing the communication by SNMP.
- Server machine 18
- Monitoring manager 19
- (Dwg.1/15)

OPD - 1998-08-07

AN - 2000-274992 [24]

PN - JP2000059385 A 20000225

PD - 2000-02-25

AP - JP19980224982 19980807

IN - SAKURAI YOSHIHARU

PA - NTT DATA CORP

TI - METHOD FOR MANAGING PLURAL SYSTEMS AT TIME OF OVERLAPPING IP ADDRESSES

AB - PROBLEM TO BE SOLVED: To provide the method for managing plural systems by which plural systems are managed by a single manager even when IP addresses are overlapped.

- SOLUTION: In this method for managing plural systems15, 16 and 17 through one monitor manager19, each system is provided with a proxy receiving server30 for mediating the communication between a server machine18 belonging to that system and the monitor manager and a system ID capable of specifying the system, to which the server machine to become the transmission destination belongs, is added to communication data in the case of communication from the monitor manager to the server machine. The proxy receiving server deletes the system ID from the communication data in the case of communication from the monitor manager to the server machine but adds the system ID capable of specifying the system, to which the server machine as a transmission source belongs, to the communication data in the case of communication from the server machine to the monitor manager.

I - H04L12/28 ;G06F13/00 ;H04L12/56

(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（A）　(11)特許出願公開番号
特開2000－59385
（P2000－59385A）
(43)公開日　平成12年２月25日(2000.2.25)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｈ０４Ｌ　12/28		Ｈ０４Ｌ　11/00	３１０Ｄ	
Ｇ０６Ｆ　13/00	３５３	Ｇ０６Ｆ　13/00	３５３Ｖ	
Ｈ０４Ｌ　12/56		Ｈ０４Ｌ　11/20	１０２Ｄ	

審査請求　未請求　請求項の数５　ＯＬ　（全 11 頁）

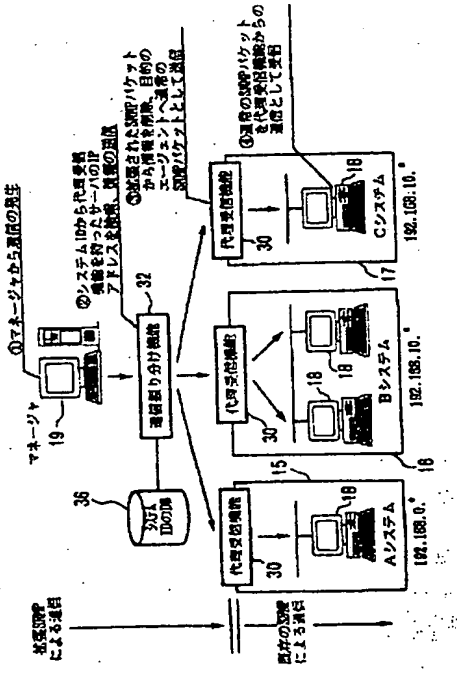
(21)出願番号　特願平10－224982

(22)出願日　平成10年８月７日(1998.8.7)

(71)出願人　000102728
株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目３番３号
(72)発明者　櫻井　義晴
東京都江東区豊洲三丁目３番３号　エヌ・ティ・テイ・データ通信株式会社内
(74)代理人　100064908
弁理士　志賀　正武　（外９名）

(54)【発明の名称】　ＩＰアドレス重複時の複数システム管理方法

(57)【要約】
【課題】　IPアドレスが重複していても、単一のマネージャによる管理が可能な複数システムの管理方法を提案する。
【解決手段】　複数のシステム１５、１６、１７を一つの監視マネージャ１９で管理する方法において、各システムに、システムに属するサーバーマシン１８と監視マネージャとの通信を仲介する代理受信サーバー３０を設け、監視マネージャからサーバーマシンへの通信の際に、通信データに、送信先となるサーバーマシンが属するシステムを特定できるシステムIDを付加し、代理受信サーバーは、監視マネージャからサーバーマシンへの通信の際には、通信データからシステムIDを削除し、サーバーマシンから監視マネージャへの通信の際には、通信データに、発信元であるサーバーマシンが属するシステムを特定できるシステムIDを付加した。



【特許請求の範囲】
【請求項1】 複数の、少なくとも1台以上のサーバーマシンを含むシステムを一つの監視マネージャで管理する方法において、
前記システムは、あるシステムに含まれるサーバーマシンのIPアドレスと、他のシステムに含まれるサーバーマシンのIPアドレスとが重複している場合に、
各システムに、このシステムに属する各サーバーマシンと前記監視マネージャとの通信を仲介する代理受信サーバーを設け、
前記監視マネージャは、この監視マネージャからサーバーマシンへの通信の際に、通信データに、送信先となるサーバーマシンが属するシステムを特定できるシステムIDを付加し、
前記代理受信サーバーは、監視マネージャからサーバーマシンへの通信の際には、通信データから、前記システムIDを削除し、サーバーマシンから監視マネージャへの通信の際には、通信データに、発信元であるサーバーマシンが属するシステムを特定できるシステムIDを付加することを特徴とするIPアドレス重複時の複数システム管理方法。
【請求項2】 前記通信は、プロトコルとしてSNMPを用い、
前記監視マネージャは、この監視マネージャからサーバーマシンへの通信の際に、前記プロトコルに、送信先となるサーバーマシンが属するシステムを特定できるシステムIDを付加し、
前記代理受信サーバーは、監視マネージャからサーバーマシンへの通信の際には、前記プロトコルから前記システムIDを削除し、サーバーマシンから監視マネージャへの通信の際には、前記プロトコルに、発信元であるサーバーマシンが属するシステムを特定できるシステムIDを付加することを特徴とする請求項1に記載のIPアドレス重複時の複数システム管理方法。
【請求項3】 前記代理受信サーバーは、重複することのないIPアドレスをもち、
前記監視マネージャと前記代理受信サーバーとの間には、監視マネージャからサーバーマシンへの通信の際に、前記システムIDを、このシステムIDに対応するシステムに設けられた代理受信サーバーのIPアドレスに変換する通信振り分けサーバーが設けられていていることを特徴とする請求項1または2に記載のIPアドレス重複時の複数システム管理方法。
【請求項4】 複数の、少なくとも1台以上のサーバーマシンを含むシステムを一つの監視マネージャで管理する方法において、
前記システムは、あるシステムに含まれるサーバーマシンのIPアドレスと、他のシステムに含まれるサーバーマシンのIPアドレスとが重複している場合に、
サーバーマシンから監視マネージャへ障害通知を行う際に、
通知元であるサーバーマシンは、障害通知データに、前記サーバーマシンが属するシステムを特定できるシステム名を付加することを特徴とするIPアドレス重複時の複数システム管理方法。
【請求項5】 前記通信は、プロトコルとしてSNMPを用い、
サーバーマシンから監視マネージャへ障害通知を行う際に、
通知元であるサーバーマシンは、前記プロトコルに、前記サーバーマシンが属するシステムを特定できるシステム名を付加することを特徴とする請求項4に記載のIPアドレス重複時の複数システム管理方法。
【発明の詳細な説明】
【0001】
【発明の属する技術分野】本発明は、分散システム運用管理方法に関する。
【0002】
【従来の技術】まず、本発明の背景となるTCP/IPとSNMPについて説明する。インターネット上の分散システムにおける通信は、TCP/IP(Transmission Control Protocol/Internet Protocol)と呼ばれるプロトコルを用いて行われる。このTCP/IPでは、IPアドレスを用いてシステム中の個々のマシンが識別されるので、インターネット上では一意なIPアドレスが用いられなければならない。IPアドレスが重複して用いられると、マシンの特定が不可能となり、通信を行うことができない。このIPアドレスの体系を表1に示す。
【表1】

表1：IPｱﾄﾞﾚｽ体系について

ｸﾗｽ	最初の1ﾊﾞｲﾄ	ﾎｽﾄ部ｻｲｽﾞ	ｻﾌﾞﾈｯﾄﾏｽｸ	目的
A	0～27	24ﾋﾞｯﾄ	255.0.0.0	通常のｱﾄﾞﾚｽ
B	128～191	16ﾋﾞｯﾄ	255.255.0.0	通常のｱﾄﾞﾚｽ
C	192～223	8ﾋﾞｯﾄ	255.255.255.0	通常のｱﾄﾞﾚｽ
D	224～239	* * *	* * *	ﾏﾙﾁｷｬｽﾄ
E	240～255	* * *	* * *	予備

【0003】また、IPアドレスには、インターネットへの接続は基本的に不可能であるが、ユーザが自由に利用

することができるアドレスが規定されている。このアドレスは、プライベートIPアドレスと呼ばれる。このプライベートIPアドレスの体系を表２に示す。

【表２】

表２：ﾌﾟﾗｲﾍﾞｰﾄIPｱﾄﾞﾚｽについて

ｸﾗｽ	利用可能ｱﾄﾞﾚｽ	ﾈｯﾄﾏｽｸ
A	10.0.0.0～10.255.255.255	255.0.0.0
B	172.16.0.0～172.32.255.255	255.255.0.0
B	192.168.0.0～192.168.255.255	255.255.0.0

【０００４】次に、SNMP(Simple Network Management Protocol)について説明する。分散システムにおいてマシンの運用管理を行う際には、監視マネージャ(以下マネージャとする)からの集中管理体制を取ることが一般的である。この管理体制を実現するために、分散している各サーバーマシンに、監視エージェント(以下エージェントとする)と呼ばれる監視アプリケーションを常駐させ監視を行う。通常エージェントはイベントドリブン方式を採用しており、エージェントで障害を検出した場合にのみ、マネージャへ情報を通知する。障害を知ったマネージャのオペレータは、詳細な情報を取得するために、マネージャからエージェントへと通信を行う。この手法は、マネージャ・エージェント間のリソースを低減するメリットがあり、広く用いられている。

【０００５】SNMPは、SNMPネットワーク上の機器の障害等を通知することを目的として設計されたTCP/IP上のプロトコルであり、障害監視等の分野で広く用いられている。SNMPによる通信は、図１（１）に示すエージェントから通信が開始されるTRAPと、図１（２）に示すマネージャから通信が開始されるGET等との２種類に分類することができる。

【０００６】SNMPのVersion1では、エージェントから通信が開始される際のコマンドであるTRAPと、マネージャから通信が開始される際のコマンドであるGET,GET NEXT,SETと、マネージャからの通信に対するエージェントからの返信であるGET RESPONSEとの合計５種類のコマンドが定義されている。これら５種類のコマンドの内容を以下に記す。

TRAP	障害時等にエージェントが発生させる通信
GET	MIB値の取得
GET NEXT	MIB値の取得(継続)
SET	MIB値のセット
GET RESPONSE	GET,GET NEXT,SETに対するエージェントからの返事

ここで、MIB(Management Information Base)とは、SNMPのエージェントが内部にもつデータベースで、装置の状態を表している。

【０００７】エージェントから通信が開始される際のコマンドであるTRAPは、機器に緊急の障害が発生した場合にその情報をマネージャに伝える。マネージャから開始される通信においては、マネージャからのリクエストに対して、該当するMIBの値をマネージャへ返す。なお、マネージャ側からこのMIBの値を変更することにより、装置の該当する機能の状態を変更することもできる。

【０００８】図２にSNMPのデータ構造を示す。SNMPは、バージョン１と、Community名２と、PDU３とで構成されている。エージェントから通信が開始される際のコマンドであるTRAPが使用されるときには、前記PDU３に、PDUタイプ４、企業ID５、エージェント・アドレス６、一般TRAP番号７、拡張TRAP番号８、発生時刻９、関連管理情報１０が入る。マネージャから通信が開始される際のコマンドであるGET,GET NEXT,SET,GET RESPONSEが使用されるときには、前記PDU３に、PDUタイプ４、リクエスト識別１１、エラー・ステータス１２、エラー位置番号１３、管理情報１４等が入る。なお、以下の各図面の説明では、同一の構成には同一の符号を付し、その説明を省略する。

【０００９】ところで、システム構築時にインターネットへの接続を前提としないシステムでは、インターネットにおいて利用可能なIPアドレスの取得に手間がかかるので、IPアドレスの割り振りについて、自由に利用することの可能なプライベートIPアドレスを利用することが多い。

【００１０】図３に、システム構築時には外部と通信する必要の無かった独立したシステムを複数構築した例を示す。図中のAシステム１５、Bシステム１６、Cシステム１７は独立したシステムである。これらのシステムには、１台以上のサーバーマシン１８が含まれている。このとき、システム設計のし易さや、構築時の手間等から、含まれているサーバーマシン１８のIPアドレス体系が全く同一であるシステムとすることが考えられる。図３では、Bシステム１６とCシステム１７とが、IPアドレス体系が全く同一となっている。

【００１１】また、システムの監視業務を行う場合に、顧客の要望に応じて監視対象システムを追加してゆくことが考えられるが、複数の顧客システムを監視する場合に、一意ではない、重複したIPアドレスが利用されていることも考えられる。

【００１２】
【発明が解決しようとする課題】上記のようなシステムに対し、構築後に他のシステムとの接続や統合的な監視が必要となった場合には、図４に示すように、各マシン１８で利用されているIPアドレスに重複があるため、監視を行うマネージャ１９は、マシン１８の一意な識別ができず、TCP/IPを利用した通信が不可能となってしまう。
【００１３】TCP/IPによる通信を可能にするには、図５に示すように、通信の代理機能すなわちPROXY２０の利用が一般的である。しかし、PROXY２０は一般的な通信路の確保を目的とした技術にすぎず、また、SNMPはその内部にエージェント特定のための情報を保持していないので、以下のような二点の問題がある。第一に、エージェントから障害通知が発生した場合、例えば図５のBシステム１６のIPアドレス192.168.10.5のエージェントと、Cシステム１７のIPアドレス192.168.10.5を持ったエージェントとの区別がつかず、マネージャ１９側で、どのエージェントからの障害通知であるかが判別できない。第二に、マネージャ１９側からの通信においても、Bシステム中のエージェントと、Cシステム中のエージェントとを判別できず、PROXY２０が通信を振り分けることができない。
【００１４】上記のような問題点に対し、従来技術では二通りの解決方法があった。第一の方法は、図６に示すように、IPアドレスの重複がある顧客システムについては、単一のマネージャによる監視を行わず、それぞれ個別のマネージャ２１、２２を用意し、お互いにネットワークを干渉させないことで監視を可能とする方法である。しかし、多数の顧客システムを同時に監視する場合には、最悪の場合、監視対象システムと同数のマネージャを用意する必要が生じ、システム面でも人員的にも非効率的な監視を行わねばならないことになる。
【００１５】第二の方法は、図７に示すように、重複が起こらないようなアドレス体系への変換テーブルを用意し、通信が生じたときに、その通信パケットに対して、発信元・送信先のIPアドレスをこのテーブルによって変換する方法である。この方法によって、単一のマネージャによる監視を可能とすることができる。しかし、この方法では、重複しているIPアドレスを全て新しいIPアドレスへ変換する必要があるので、重複しているIPアドレスと同じ数だけの新たなIPアドレスを用意する必要がある。すると、監視対象システムが増加した場合、IPアドレスが不足し、対応できなくなる可能性がある。
【００１６】本発明は、上記の問題を解決するためになされたもので、単一のマネージャによる監視を可能とし、かつ使用されているIPアドレスが重複していても、新しいIPアドレスへ変換する必要がない方法を提案するものである。
【００１７】
【課題を解決するための手段】請求項１に記載の発明は、複数の、少なくとも１台以上のサーバーマシンを含むシステムを一つの監視マネージャで管理する方法において、前記システムは、あるシステムに含まれるサーバーマシンのIPアドレスと、他のシステムに含まれるサーバーマシンのIPアドレスとが重複している場合に、各システムに、このシステムに属する各サーバーマシンと前記監視マネージャとの通信を仲介する代理受信サーバーを設け、前記監視マネージャは、この監視マネージャからサーバーマシンへの通信の際に、通信データに、送信先となるサーバーマシンが属するシステムを特定できるシステムIDを付加し、前記代理受信サーバーは、監視マネージャからサーバーマシンへの通信の際には、通信データから、前記システムIDを削除し、サーバーマシンから監視マネージャへの通信の際には、通信データに、発信元であるサーバーマシンが属するシステムを特定できるシステムIDを付加することを特徴とするIPアドレス重複時の複数システム管理方法である。
【００１８】請求項２に記載の発明は、前記通信は、プロトコルとしてSNMPを用い、前記監視マネージャは、この監視マネージャからサーバーマシンへの通信の際に、前記プロトコルに、送信先となるサーバーマシンが属するシステムを特定できるシステムIDを付加し、前記代理受信サーバーは、監視マネージャからサーバーマシンへの通信の際には、前記プロトコルから前記システムIDを削除し、サーバーマシンから監視マネージャへの通信の際には、前記プロトコルに、発信元であるサーバーマシンが属するシステムを特定できるシステムIDを付加することを特徴とする請求項１に記載のIPアドレス重複時の複数システム管理方法である。
【００１９】請求項３に記載の発明は、前記代理受信サーバーは、重複することのないIPアドレスをもち、前記監視マネージャと前記代理受信サーバーとの間には、監視マネージャからサーバーマシンへの通信の際に、前記システムIDを、このシステムIDに対応するシステムに設けられた代理受信サーバーのIPアドレスに変換する通信振り分けサーバーが設けられていていることを特徴とする請求項１または２に記載のIPアドレス重複時の複数システム管理方法である。
【００２０】請求項４に記載の発明は、複数の、少なくとも１台以上のサーバーマシンを含むシステムを一つの監視マネージャで管理する方法において、前記システムは、あるシステムに含まれるサーバーマシンのIPアドレスと、他のシステムに含まれるサーバーマシンのIPアドレスとが重複している場合に、サーバーマシンから監視マネージャへ障害通知を行う際に、通知元であるサーバーマシンは、障害通知データに、前記サーバーマシンが属するシステムを特定できるシステム名を付加することを特徴とするIPアドレス重複時の複数システム管理方法である。

【００２１】請求項５に記載の発明は、前記通信は、プロトコルとしてSNMPを用い、サーバーマシンから監視マネージャへ障害通知を行う際に、通知元であるサーバーマシンは、前記プロトコルに、前記サーバーマシンが属するシステムを特定できるシステム名を付加することを特徴とする請求項４に記載のIPアドレス重複時の複数システム管理方法である。

【００２２】

【発明の実施の形態】まず、図９を参照して、本発明の第１実施形態、すなわちサーバーマシン１８からマネージャ１９への障害の通知を行う場合の構成を説明する。図示したAシステム１５、Bシステム１６、Cシステム１７のように分散したシステムに属するサーバーマシン１８を、単一のマネージャ１９で集中的に管理するために、各サーバーマシン１８に、エージェントと呼ばれる監視アプリケーションを常駐させ監視を行う。エージェントは、このエージェントが常駐するサーバーマシン１８の障害を検出した場合に、マネージャ１９へ障害情報を通知する。以後、エージェントが常駐するサーバーマシン１８を、単に、エージェント１８と呼ぶ。

【００２３】各システムに属するエージェント１８は、システム内においては一意のIPアドレスをもつが、システム外には重複するIPアドレスがある場合がある。本実施形態においては、Bシステムと、Cシステムとは、IPアドレス体系が全く同一となっている。

【００２４】Aシステム１５、Bシステム１６、Cシステム１７には、これらのシステムに属するエージェント１８とマネージャ１９との通信を仲介する、代理受信機能３０がそれぞれ設けられている。また、マネージャ１９は、通信先選択マネージャ３１を介して、各システムの代理受信機能３０に接続されている。さらに、通信先選択マネージャ３１には、仮想－実空間変換テーブルが記憶されているデータベース３５が接続されている。

【００２５】次に、本実施形態の動作を説明する。マネージャ１９とエージェント１８との間の通信は、SNMPと呼ばれるプロトコルによって行う。エージェント１８は障害を検出した場合に、マネージャ１９へ障害情報を通知するが、このとき、SNMPにおいては、TRAPと呼ばれるコマンドを使用する。例えば、Cシステム１７のあるエージェント１８が障害を検出すると、この情報をTRAP通信として、Cシステム１７の代理受信機能３０を介して、通信先選択マネージャ３１に通知する。

【００２６】エージェント１８は、TRAP送信時に、図８に示すSNMPのデータ構造中の、関連管理情報１０に、システム名２３、ホスト名２４、大項目２５、中項目２６、小項目２７、状態２８、値２９といった階層化された障害情報を入れる。図８には、一例として、A商社のホスト(1)においてハードディスクの容量が７０パーセントとなった場合の警告を示す。このとき、システム名２３=A-SYOUSYA、ホスト名２４=HOST(1)、大項目２５=HD、中項目２６=DISK(1)、小項目２７=USAGE、状態２８=WARNING、値２９=70となる。なお、階層化された障害情報の例を表３に示す。

【表３】

表３：ｼｽﾃﾑの障害を一意に識別するための情報の階層化の例

ｼｽﾃﾑ名	ﾎｽﾄ名	大項目	中項目	小項目	状態	値
A商社	HOST(1)	CPU	CPU(1)	負荷	Normal	10
				負荷平均	Normal	30
				⋮	⋮	⋮
			CPU(2)	負荷	Normal	⋮
				⋮	⋮	⋮
		HD	DISK(1)	使用容量	Warning	50
				負荷率	⋮	⋮
				⋮	⋮	⋮
			DISK(2)	⋮	⋮	⋮
		MEMORY	MEMORY(1)	使用容量	Normal	40
				⋮	⋮	⋮
		DB	DB(1)	⋮	⋮	⋮
				⋮	⋮	⋮
			DB(2)	⋮	⋮	80
	HOST(2)	CPU	CPU(1)	⋮	⋮	50
		⋮	⋮	⋮	⋮	⋮
		⋮	⋮	⋮	⋮	⋮
B商社	HOST(3)	CPU	CPU(1)	負荷	Normal	40
		⋮	⋮	⋮	⋮	⋮
	⋮	⋮	⋮	⋮	⋮	⋮

【００２７】通信先選択マネージャ３１は、前記の階層化された障害情報を受信すると、この情報に含まれるシステム名２３、ホスト名２４から発信元のエージェント１８を認識し、さらに大項目２５、中項目２６、小項目２７、状態２８、値２９から障害を特定する。後に続く動作として、マネージャ１９は障害情報のシンボルを変化させるが、通信先選択マネージャ３１は、どのシンボルを変化させるかを、データベース３５を参照して決定する。

【００２８】この決定をもとに、マネージャ１９は、図

１０に示す該当する障害情報のシンボルを変化させ、障害情報の表示を行う。以上の方法により、マネージャ１９のオペレータは、エージェント１８のIPアドレスに重複がある場合であっても、発信元のエージェントを特定できる。

【００２９】次に、図１２、および図１４を用いて、本発明の第２実施形態、すなわちマネージャ１９からエージェント１８へのリクエスト通信、およびこれに対するエージェント１８からマネージャ１９への返信を行う場合の構成を説明する。

【００３０】前記の障害を知ったマネージャ１９のオペレータは、詳細な情報を取得するために、マネージャ１９からエージェント１８へとリクエスト通信を行い、これに対して、エージェント１８は詳細な情報をマネージャ１９へ返信する。図１２はマネージャ１９からエージェント１８への通信を示し、図１４はこれに対するエージェント１８からマネージャ１９への返信を示しているが、用いている構成は同一である。

【００３１】マネージャ１９は、通信振り分け機能３２を介して、各システムにそれぞれ設けられた代理受信機能３０と接続されている。また、前記通信振り分け機能３２には、システムIDのデータベース３６が接続されている。また、代理受信機能３０には、相互に重複のない、一意のIPアドレスが付けられている。

【００３２】本実施形態のSNMPにおいては、GET,GET NEXT,SET,GET RESPONSEといったコマンドが使用される。また、SNMPのデータ構造には、図１１に示すように、エージェントIPアドレス３３と、システムID３４とが付加される。エージェントIPアドレス３３とは、各エージェント１８に付けられたIPアドレスである。システムID３４とは、監視対象システム１５、１６、１７に付けられた一意のID番号である。

【００３３】前記システムIDのデータベース３６には、表４に示すような、システムID３４を対応する代理受信機能３０のIPアドレスに変換するためのテーブルが記憶されている。

【表４】

表４：通信振分け機能が管理するシステムID－代理受信機能のIPｱﾄﾞﾚｽ変換ﾃｰﾌﾞﾙ

ｼｽﾃﾑID	代理受信機能のIPｱﾄﾞﾚｽ
1	10.15.1.10
2	10.15.1.11
3	10.15.1.24
4	10.15.1.33

上記以外の構成は、第１実施形態と同様である。

【００３４】次に、図１２、および図１３のフローチャートを用いて、マネージャ１９からエージェント１８へのリクエスト通信(GET等)の動作を説明する。なお、以下の文中に示すＳ１～Ｓ８は、図１３のステップを示す。

【００３５】マネージャ１９からの通信が発生すると（Ｓ１）、送信データとして、エージェントIPアドレス３３とシステムID３４とが付加された拡張SNMPパケットが作成される（Ｓ２）。このパケットが通信振り分け機能３２に送られると、この通信振り分け機能３２は、システムIDのデータベース３６に記憶されている変換テーブルを参照し、システムID３４を代理受信機能３０のIPアドレスに変換する（Ｓ３）。そして、このIPアドレスが登録されたものであるかが確認され（Ｓ４）、登録されていなければ、通信障害をマネージャ１９に通知する（Ｓ５）。登録されていれば、変換されたIPアドレスをもつ代理受信機能３０へパケットを送信する（Ｓ６）。

【００３６】該当するIPアドレスをもつ代理受信機能３０が、前記拡張SNMPパケットを受信すると、このパケットからエージェントIPアドレス３３とシステムID３４とを削除し（Ｓ７）、送信先のエージェント１８へ、通常のSNMPパケットとして送信する。そして、エージェント１８は、通常のSNMPパケットを受信する（Ｓ８）。従って、この方法では、エージェント１８は通常のSNMPパケットが受信できる機能をもっていればよいので、従来からあるエージェントに対して、特別な変更をする必要はない。

【００３７】次に、図１４、および図１５のフローチャートを用いて、マネージャ１９からのリクエストに対する、エージェント１８からマネージャ１９への返信(GET RESPONSE)の動作を説明する。なお、以下の文中に示すＳ９～Ｓ１６は、図１５のステップを示す。

【００３８】例えば、Cシステム１７に属するあるエージェントからの通信が発生すると（Ｓ９）、ここから送信された通常のSNMPパケットは、このエージェント１８が属するCシステム１７の代理受信機能３０によって受信される。代理受信機能３０は、受信したパケットに、発信元エージェント１８のエージェントIPアドレス３３およびシステムID３４を付加し、拡張SNMPパケットとして（Ｓ１０）、通信振り分け機能３２へ送信する。

【００３９】拡張SNMPパケットを受信した通信振り分け機能３２は、パケットに付加されたシステムID３４が、システムIDのデータベース３６に登録された正しいものかどうか確認し、登録されていない不正なものであれば、通信障害をマネージャ１９に通知する（Ｓ１１～Ｓ１４）。登録された正しいものであれば、パケットをマネージャ１９へ送る（Ｓ１５）。そして、マネージャ１９は、拡張SNMPパケットを受信する（Ｓ１６）。従って、エージェント１８からの返信には、プロトコル中にシステムID３４が付加されているので、マネージャ１９は、どのエージェント１８からの返信であるかを一意に特定することができる。

【００４０】

【発明の効果】本発明によると、IPアドレスが重複して

いる複数のシステムを単一のマネージャで管理することが可能になった。従って、効率の良い集中的な管理を行うことができるようになった。また、システムの監視業務を行う場合に、顧客の要望等に応じて監視対象システムを追加して、重複したIPアドレスが利用されていたとしても、複数のマネージャを設置する必要はなく、既存資産が活用でき、コストが増加することはない。さらに、このとき、既に多数設置されているエージェントに対して、IPアドレスの変更や、拡張されたSNMPによる通信への対応などの特別な変更をする必要はなく、ユーザは本発明の仕組みを認識する必要もない。

【図面の簡単な説明】

【図１】　SNMPによる通信を示す図。

【図２】　従来のSNMPプロトコルを示す図。

【図３】　IPアドレスの重複したシステムを示す図。

【図４】　IPアドレスの重複により通信が不可能となる例を示す図。

【図５】　従来技術であるPROXY機能により通信を可能とする例を示す図。

【図６】　従来技術である複数マネージャを利用する方法を示す図。

【図７】　従来技術であるアドレス変換による方法を示す図。

【図８】　本発明の第１実施形態によるSNMP TRAPのPDUに対する情報のマッピング例を示す図。

【図９】　本発明の第１実施形態によるエージェントからマネージャへの障害の通知を示す図。

【図１０】　本発明の第１実施形態による障害情報のシンボルの状態変化を示す図。

【図１１】　本発明の第２実施形態による拡張されたSNMPプロトコルを示す図。

【図１２】　本発明の第２実施形態によるマネージャからエージェントへのリクエスト通信を示す図。

【図１３】　マネージャからエージェントへのリクエスト通信のフローチャート。

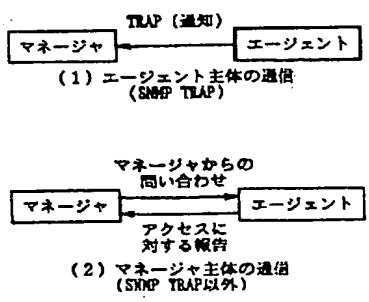
【図１４】　本発明の第２実施形態によるマネージャのリクエストに対するエージェントからマネージャへの返信を示す図。

【図１５】　マネージャのリクエストに対するエージェントからマネージャへの返信のフローチャート。

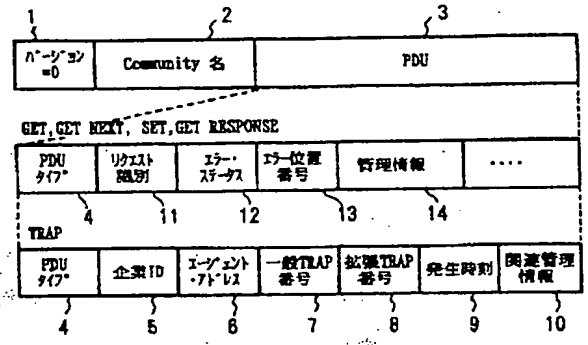
【符号の説明】

１　バージョン	２　Community名
３　PDU	４　PDUタイプ
５　企業ID	６　エージェント・アドレス
７　一般TRAP番号	８　拡張TRAP番号
９　発生時刻	１０　関連管理情報
１１　リクエスト識別	１２　エラー・ステータス
１３　エラー位置番号	１４　管理情報
１５　Aシステム	１６　Bシステム
１７　Cシステム	１８　サーバーマシン(エージェント)
１９　マネージャ	２０　PROXY
２１　マネージャ	２２　マネージャ
２３　システム名	２４　ホスト名
２５　大項目	２６　中項目
２７　小項目	２８　状態
２９　値	３０　代理受信機能
３１　通信先選択マネージャ	３２　通信振り分け機能
３３　エージェントIPアドレス	３４　システムID
３５　データベース	３６　システムIDのデータベース

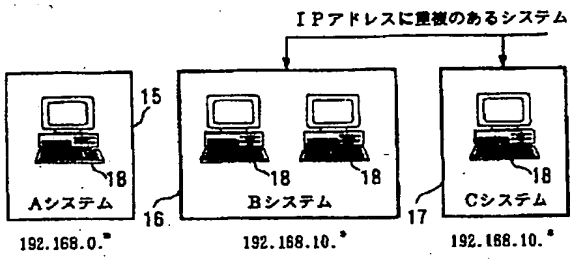
【図１】



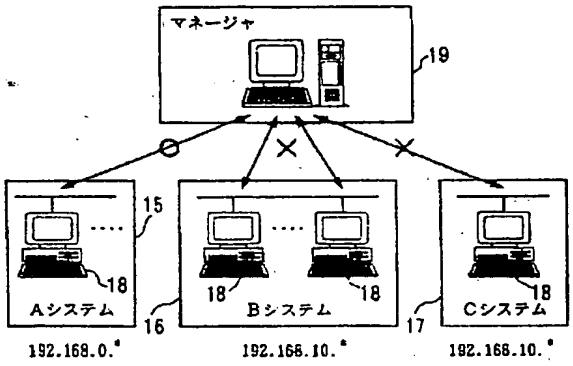
【図２】



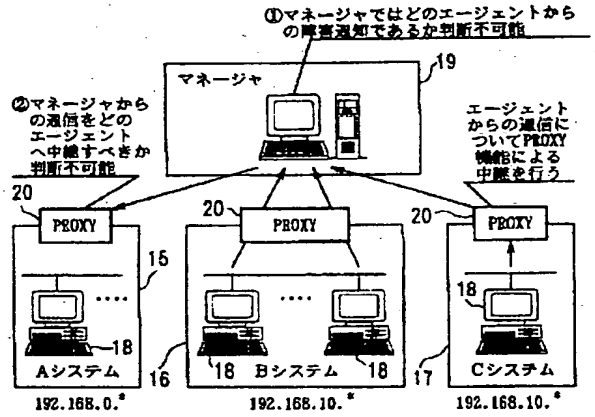
【図3】



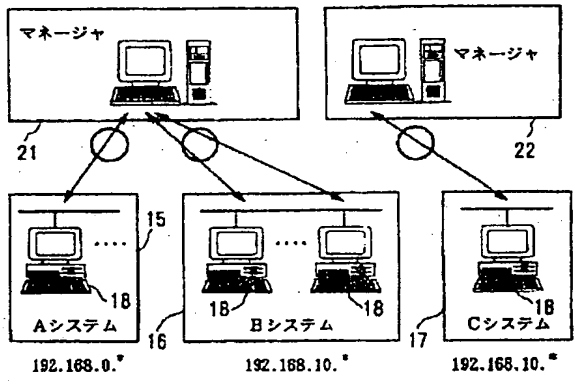
【図4】



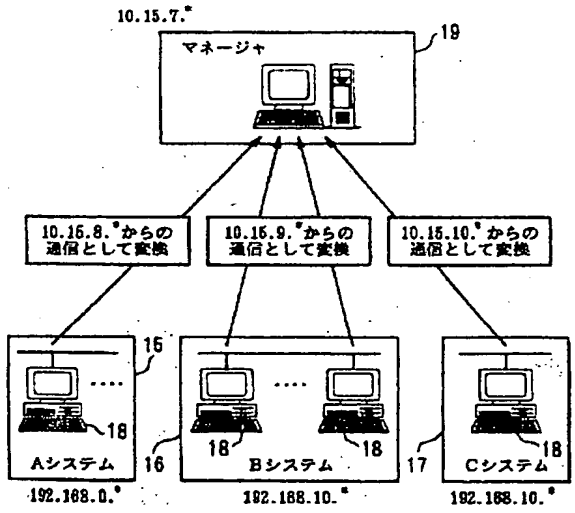
【図5】



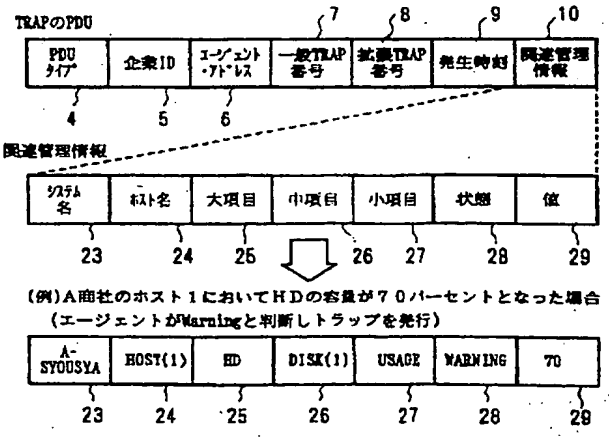
【図6】



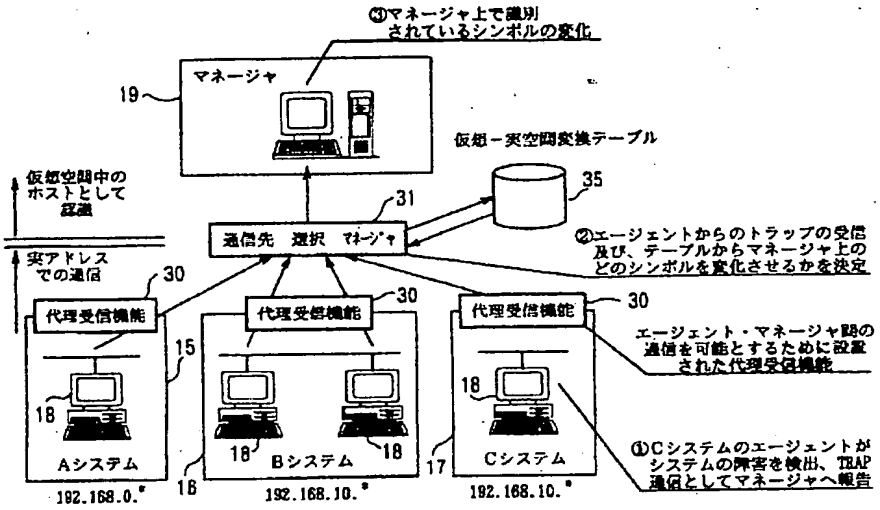
【図7】



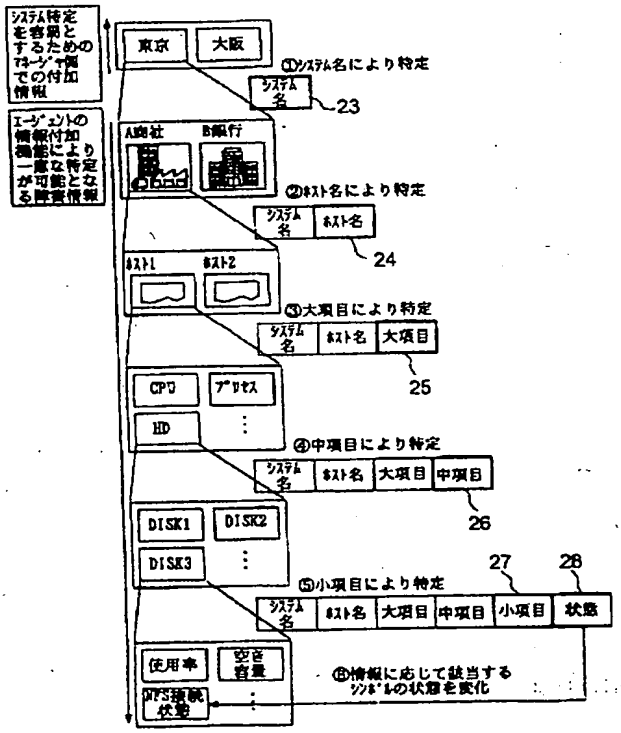
【図8】



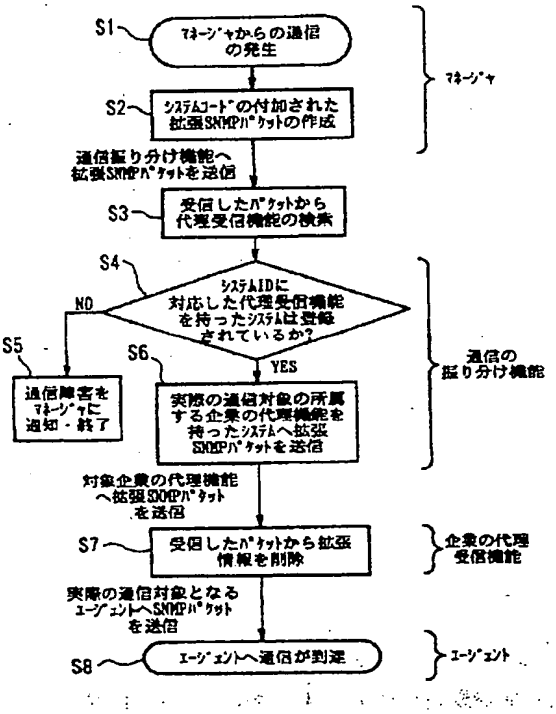
【図9】


③マネージャ上で識別されているシンボルの変化
マネージャ
19
仮想－実空間変換テーブル
35
31
仮想空間中のホストとして認識
実アドレスでの通信
通信先 選択 ﾏﾈｰｼﾞｬ
②エージェントからのトラップの受信及び、テーブルからマネージャ上のどのシンボルを変化させるかを決定
30
代理受信機能
30
代理受信機能
30
代理受信機能
エージェント・マネージャ間の通信を可能とするために設置された代理受信機能
15
18
Aシステム
192.168.0.*
16
18
18
Bシステム
192.168.10.*
17
18
Cシステム
192.168.10.*
①Cシステムのエージェントがシステムの障害を検出、TRAP通信としてマネージャへ報告

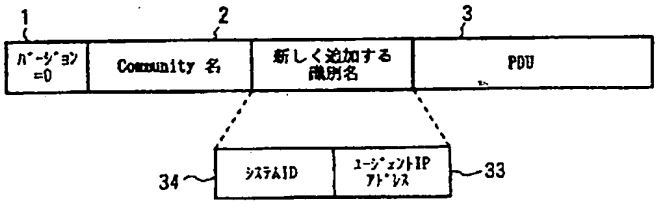
【図10】


ｼｽﾃﾑ特定を容易とするためのﾏﾈｰｼﾞｬ側での付加情報
ｴｰｼﾞｪﾝﾄの情報付加機能により一意な特定が可能となる障害情報
東京
大阪
①ｼｽﾃﾑ名により特定
ｼｽﾃﾑ名
23
A銀社
B銀行
②ﾎｽﾄ名により特定
ｼｽﾃﾑ名
ﾎｽﾄ名
24
ﾎｽﾄ1
ﾎｽﾄ2
③大項目により特定
ｼｽﾃﾑ名
ﾎｽﾄ名
大項目
25
CPU
ｱﾌﾟﾘｹｰｼｮﾝ
HD
④中項目により特定
ｼｽﾃﾑ名
ﾎｽﾄ名
大項目
中項目
26
DISK1
DISK2
DISK3
27
28
⑤小項目により特定
ｼｽﾃﾑ名
ﾎｽﾄ名
大項目
中項目
小項目
状態
使用率
空き容量
NFS接続状態
⑥情報に応じて該当するｼﾝﾎﾞﾙの状態を変化

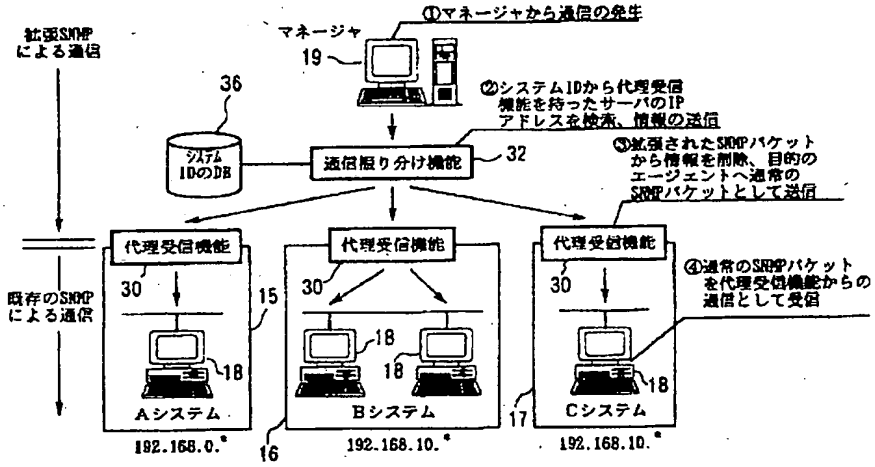
【図13】


S1
ﾏﾈｰｼﾞｬからの通信の発生
S2
ｼｽﾃﾑｺｰﾄﾞの付加された拡張SNMPﾊﾟｹｯﾄの作成
ﾏﾈｰｼﾞｬ
通信振り分け機能へ拡張SNMPﾊﾟｹｯﾄを送信
S3
受信したﾊﾟｹｯﾄから代理受信機能の検索
S4
ｼｽﾃﾑIDに対応した代理受信機能を持ったｼｽﾃﾑは登録されているか?
NO
YES
S5
通信障害をﾏﾈｰｼﾞｬに通知・終了
S6
実際の通信対象の所属する企業の代理機能を持ったｼｽﾃﾑへ拡張SNMPﾊﾟｹｯﾄを送信
通信の振り分け機能
対象企業の代理機能へ拡張SNMPﾊﾟｹｯﾄを送信
S7
受信したﾊﾟｹｯﾄから拡張情報を削除
企業の代理受信機能
実際の通信対象となるｴｰｼﾞｪﾝﾄへSNMPﾊﾟｹｯﾄを送信
S8
ｴｰｼﾞｪﾝﾄへ通信が到達
ｴｰｼﾞｪﾝﾄ

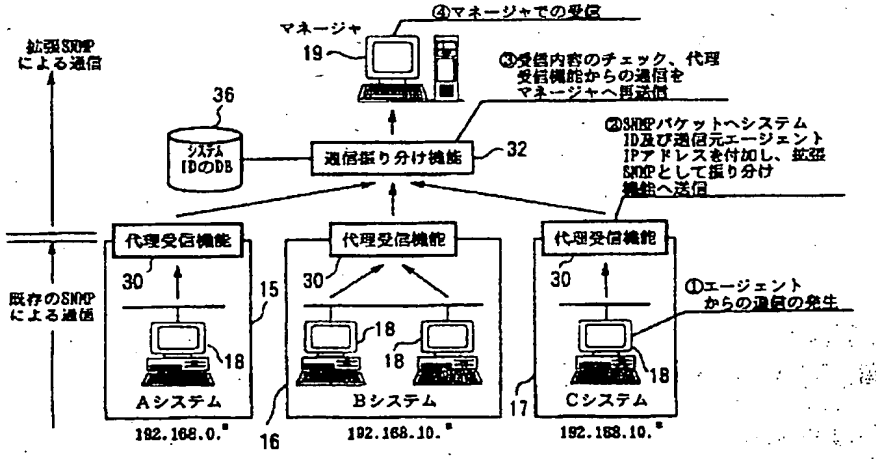
【図１１】


1
2
3
ﾊﾞｰｼﾞｮﾝ =0
Community 名
新しく追加する識別名
PDU
34
ｼｽﾃﾑID
ｴｰｼﾞｪﾝﾄIP ｱﾄﾞﾚｽ
33

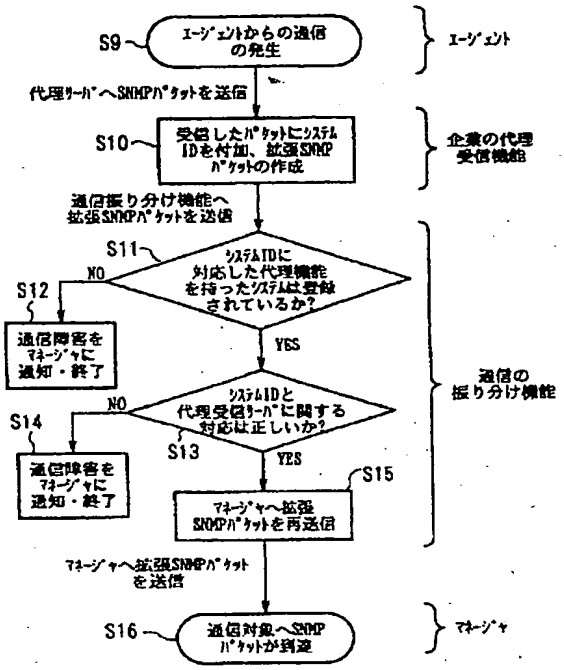
【図１２】


拡張SNMP による通信
既存のSNMP による通信
マネージャ
19
①マネージャから通信の発生
②システムIDから代理受信機能を持ったサーバのIPアドレスを検索、情報の送信
③拡張されたSNMPパケットから情報を削除、目的のエージェントへ通常のSNMPパケットとして送信
④通常のSNMPパケットを代理受信機能からの通信として受信
36
ｼｽﾃﾑ IDのDB
通信振り分け機能
32
代理受信機能
30
15
16
17
18
Aシステム
Bシステム
Cシステム
192.168.0.*
192.168.10.*
192.168.10.*

【図１４】


拡張SNMP による通信
既存のSNMP による通信
マネージャ
19
④マネージャでの受信
③受信内容のチェック、代理受信機能からの通信をマネージャへ再送信
②SNMPパケットへシステムID及び通信元エージェントIPアドレスを付加し、拡張SNMPとして振り分け機能へ送信
①エージェントからの通信の発生
36
ｼｽﾃﾑ IDのDB
通信振り分け機能
32
代理受信機能
30
15
16
17
18
Aシステム
Bシステム
Cシステム
192.168.0.*
192.168.10.*
192.168.10.*

【図15】


S9
エージェントからの通信の発生
エージェント
代理サーバへSNMPパケットを送信
S10
受信したパケットにシステムIDを付加、拡張SNMPパケットの作成
企業の代理受信機能
通信振り分け機能へ拡張SNMPパケットを送信
S11
システムIDに対応した代理機能を持ったシステムは登録されているか?
NO
S12
通信障害をマネージャに通知・終了
YES
システムIDと代理受信サーバに関する対応は正しいか?
NO
S14
通信障害をマネージャに通知・終了
S13
YES
S15
マネージャへ拡張SNMPパケットを再送信
通信の振り分け機能
マネージャへ拡張SNMPパケットを送信
S16
通信対象へSNMPパケットが到達
マネージャ